

Continuous-variable blind quantum computation

Tomoyuki Morimae*

*Controlled Quantum Dynamics Theory Group,
Imperial College London, London SW7 2BW, United Kingdom*

(Dated: August 3, 2012)

Abstract

Blind quantum computation is a secure delegated quantum computing protocol where Alice who does not have sufficient quantum technology at her disposal delegates her computation to Bob who has a fully-fledged quantum computer in such a way that Bob cannot learn anything about Alice's input, output, and algorithm. Protocols of blind quantum computation have been proposed for several qubit measurement-based computation models, such as the graph state model, the Affleck-Kennedy-Lieb-Tasaki model, and the Raussendorf-Harrington-Goyal topological model. Here, we consider blind quantum computation for the continuous-variable measurement-based model. We show that blind quantum computation is possible for the infinite squeezing case. We also show that the finite squeezing causes no additional problem in the blind setup apart from the one inherent to the continuous-variable measurement-based quantum computation.

*Electronic address: morimae@gmail.com

I. INTRODUCTION

When scalable quantum computers are realized, they will be used in “cloud computing style” since only limited number of people will be able to possess quantum computers. Blind quantum computation [1–10] provides a solution to the issue of the client’s security in such a cloud quantum computation. Blind quantum computation is a new secure protocol which enables Alice who does not have enough quantum technology to delegate her computation to Bob who has a fully-fledged quantum computer in such a way that Bob cannot learn anything about Alice’s input, output, and algorithm. A protocol of the unconditionally secure universal blind quantum computation for almost classical Alice was first proposed in Ref. [3] by using the measurement-based quantum computation (MBQC) on the cluster state [11–13], and later generalized to other resource states such as the Affleck-Kennedy-Lieb-Tasaki state [5, 14, 15] and the three-dimensional Raussendorf-Harrington-Goyal state [16–20] which enables the topological protection [8, 9]. A subroutine which eases Alice’s burden was invented [6]. Also, a verification scheme which tests Bob’s honesty was proposed [9]. The proof-of-principle experiment of the original protocol [3] was realized in an optical system [7].

In this paper, we consider the continuous-variable (CV) version of the blind quantum computation. The CV cluster MBQC was proposed in Refs. [21, 22]. There,

$$|+\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

state of a single qubit is replaced with the zero momentum state $|0\rangle_p$ of a single mode (qumode), and the two-mode gate $e^{iq\otimes q}$ plays the role of the qubit Controlled-Z gate,

$$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z.$$

Experimental demonstrations of building blocks of the CV cluster MBQC were already achieved [23–27].

We show that blind quantum computation is possible in the infinite squeezing case. We also consider the finite squeezing case, and show that the finite squeezing causes no problem apart from the additional errors which come from the redundancy of gates required for the blindness. Since these errors are those even the non-blind CV MBQC has to cope with for its scalability, we conclude that the finite squeezing does not cause any fundamental problem in principle.

This paper is organized as follows. In the next section we will briefly review the CV cluster MBQC. We also review the qubit blind quantum computation in Sec. III. Then we explain our protocol in Sec. IV, and show its correctness (Sec. V) and blindness (Sec. VI). Discussions are given in Sec. VII.

II. CV CLUSTER MBQC

Let us briefly review the CV cluster MBQC proposed in Refs. [21, 22]. Let q and p be the quadrature “position” and “momentum” operators, respectively, satisfying the canonical commutation relation

$$[q, p] = i.$$

We also define the Weyl-Heisenberg operators

$$\begin{aligned} X(s) &\equiv \exp[-isp], \\ Z(s) &\equiv \exp[isq], \end{aligned}$$

with $s \in \mathbb{R}$, where

$$\begin{aligned} X(s)|t\rangle_q &= |t+s\rangle_q, \\ Z(s)|t\rangle_p &= |t+s\rangle_p. \end{aligned}$$

Here, $|t\rangle_q$ and $|t\rangle_p$ are eigenvectors of q and p with the eigenvalue t , respectively. They satisfy

$$\begin{aligned} X(s)Z(t) &= e^{-ist}Z(t)X(s), \\ qX(s) &= X(s)(q+s), \\ pZ(s) &= Z(s)(p+s). \end{aligned}$$

These Weyl-Heisenberg operators are CV analog of the qubit Pauli operators. The Fourier transform operator F is defined by

$$F \equiv \exp\left[i(q^2 + p^2)\frac{\pi}{4}\right],$$

with

$$F|s\rangle_q = |s\rangle_p.$$

This operator is the CV analog of the qubit Hadamard operator. However, special cares are needed because F is not Hermitian and

$$\begin{aligned}
F^2|s\rangle_q &= |-s\rangle_q, \\
F^2|s\rangle_p &= |-s\rangle_p, \\
F^4 &= I, \\
F^\dagger q F &= -p, \\
F^\dagger p F &= q, \\
Z(m)F &= FX(m), \\
X(m)F &= FZ(-m).
\end{aligned}$$

The CV version of the Controlled- Z gate are defined by

$$CZ \equiv \exp(iq \otimes q).$$

Note that we use the symbol CZ for both qubit CZ and CV CZ . But no confusion will occur because they can be distinguished from the context. The CV version of the Controlled- X gate is defined by

$$CX \equiv \exp(-iq \otimes p).$$

The elementary block of the CV cluster MBQC is the teleportation gate given in Fig. 1. Here,

$$D_q^f \equiv \exp[if(q)],$$

and f is a polynomial of q . Note that D_q^f and D_p^f are obtained from FD_q^f , since

$$\begin{aligned}
(FD_q^0)^3 FD_q^f &= D_q^f, \\
(FD_q^0)^2 (FD_{-q}^f) (FD_q^0) &= D_p^f.
\end{aligned}$$

Furthermore, $e^{isq^k/k}$ ($k = 1, 2, 3$) and $e^{isp^k/k}$ ($k = 1, 2, 3$) are single-mode universal [28]. Hence

$$R_q(v) \equiv F \exp \left[i \left(aq + b \frac{q^2}{2} + c \frac{q^3}{3} \right) \right]$$

is single-mode universal, where $v = (a, b, c)$. Addition of CZ enables all multi-mode universality.

Let us explain how to compensate the byproduct error $X(m)$. Note that

$$\begin{aligned} R_q(v)X(m) &= Z(m)R_{q+m}(v), \\ &= Z(m)R_q(M_mv), \end{aligned}$$

where

$$M_m = \begin{pmatrix} 1 & m & m^2 \\ 0 & 1 & 2m \\ 0 & 0 & 1 \end{pmatrix}$$

and its inverse is

$$M_m^{-1} = \begin{pmatrix} 1 & -m & m^2 \\ 0 & 1 & -2m \\ 0 & 0 & 1 \end{pmatrix}.$$

Therefore, if we want to implement $R_q(v)$, and if there is the byproduct $X(m)$, we have only to implement $R_q(M_m^{-1}v)$. Furthermore, we can show

$$\begin{aligned} CZ(X(m) \otimes I) &= (X(m) \otimes Z(m))CZ, \\ CZ(I \otimes X(m)) &= (Z(m) \otimes X(m))CZ. \end{aligned}$$

Therefore, the byproducts can be sent forward through CZ gates. In short, Fig. 2 (a) is universal if the feed-forwarding is appropriately done.

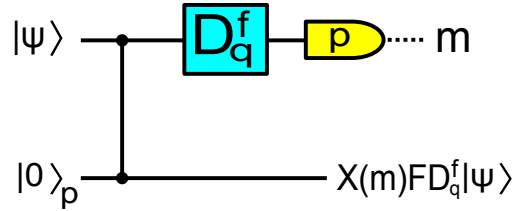


FIG. 1: (Color online.) The CV teleportation gate.

The application of D_q^f followed by the measurement of p is equivalent to the measurement of the observable $(D_q^f)^\dagger p D_q^f$. Therefore, to implement the gate e^{isq} in Fig. 1, we measure

$$e^{-isq} p e^{isq} = p + s.$$

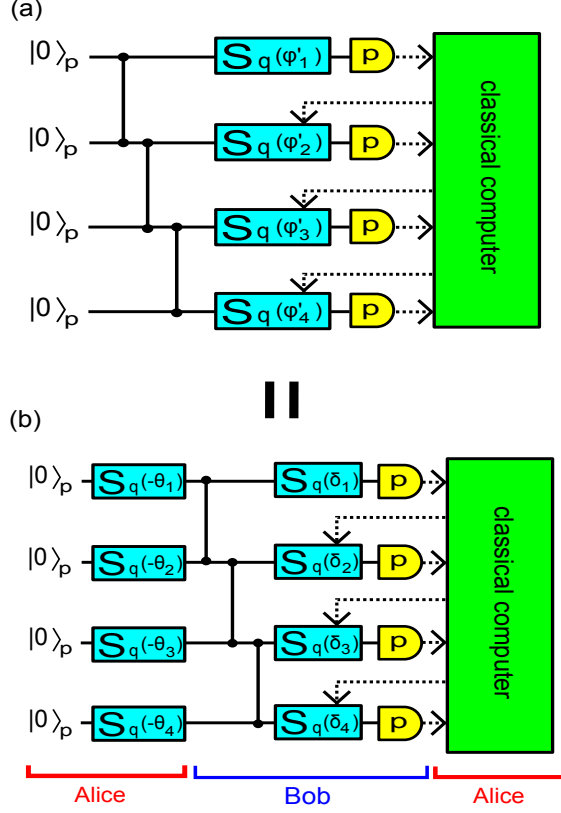


FIG. 2: (Color online.) (a): $S_q(\phi)$ stands for $F^\dagger R_q(\phi)$. This circuit is universal if $\{\phi'_j\}$ are appropriately chosen according to the previous measurement results. (b): The blind version of (a). Obviously, S_q 's commute with CZ 's, and therefore (b) is equivalent to (a).

It can be measured easily with a homodyne detection. To implement the gate $e^{isq^2/2}$ in Fig. 1, we measure

$$e^{-isq^2/2} p e^{isq^2/2} = p + sq.$$

It can also be measured with a homodyne detection in a rotated quadrature basis. In principle, the gate $e^{isq^3/3}$ can be implemented in Fig. 1 by measuring

$$e^{-isq^3/3} p e^{isq^3/3} = p + sq^2.$$

Finally, let us notice that the zero-momentum state $|0\rangle_p$ is not realistic, and normally $|0\rangle_p$ is approximated by the finitely squeezed vacuum state

$$|0, \Omega\rangle_p = \frac{1}{(\pi\Omega^2)^{1/4}} \int dp e^{-\frac{p^2}{2\Omega^2}} |p\rangle_p.$$

This finite squeezing causes errors in the CV cluster MBQC [21, 22].

III. BLIND QUANTUM COMPUTATION

Let us also briefly review the basic idea of the original blind quantum computation protocol of Ref. [3]. For details, see Refs. [3, 5–10]. Alice, the client, has a quantum device which emits randomly-rotated single qubit states and a classical computer. Bob, the server, has a full quantum power. Let us assume that Alice wants to perform the cluster MBQC on the N -qubit graph state $|G\rangle$ with measurement angles $\{\phi_j\}_{j=1}^N$. If Alice sends Bob $\{\phi_j\}_{j=1}^N$, and Bob creates $|G\rangle$, the delegated quantum computation is of course possible. However, obviously, in this case Bob can learn Alice's privacy. Hence they run the following protocol:

1. Alice sends Bob N randomly-rotated single-qubit states $\{|+\theta_j\rangle\}_{j=1}^N$, where

$$|+\theta\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle) = e^{-iZ\theta/2}|+\rangle$$

and

$$\theta_j \in \left\{ \frac{k\pi}{4} \mid k = 0, 1, \dots, 7 \right\}$$

is a random angle which is hidden to Bob.

2. Bob applies CZ gates among them. Since CZ commutes with $e^{-iZ\theta/2}$, what Bob obtains is

$$\begin{aligned} & \left(\bigotimes_{e \in E} CZ_e \right) \left(\bigotimes_{j=1}^N e^{-iZ_j\theta_j/2} \right) |+\rangle^{\otimes N} \\ &= \left(\bigotimes_{j=1}^N e^{-iZ_j\theta_j/2} \right) \left(\bigotimes_{e \in E} CZ_e \right) |+\rangle^{\otimes N} \\ &= \left(\bigotimes_{j=1}^N e^{-iZ_j\theta_j/2} \right) |G\rangle, \end{aligned}$$

where E is the set of edges of G , and the subscript j of Z_j means the operator acts on j th qubit.

3. For $j = 1$ to N in turn:

- (a) Alice sends Bob

$$\delta_j \equiv \theta_j + \phi'_j + r_j\pi,$$

where ϕ'_j is the modification of ϕ_j which includes appropriate feedforwardings (byproduct corrections) and $r_j \in \{0, 1\}$ is a random binary.

- (b) Bob does the measurement in the $\{|\pm_{\delta_j}\rangle\}$ basis, and returns the measurement result to Alice.

It was shown in Ref. [3] that this protocol is correct. Here, correct means that if Bob is honest Alice obtains the correct outcome. In fact, if Bob measures k th qubit in the $\{|\pm_{\delta_k}\rangle\}$ basis,

$$\begin{aligned}
& \langle \pm_{\delta_k} | \left(\bigotimes_{j=1}^N e^{-iZ_j \theta_j / 2} \right) | G \rangle \\
&= \langle \pm | e^{iZ_k \delta_k / 2} \left(\bigotimes_{j=1}^N e^{-iZ_j \theta_j / 2} \right) | G \rangle \\
&= \left(\bigotimes_{j \neq k} e^{-iZ_j \theta_j / 2} \right) \langle \pm | e^{iZ_k \delta_k / 2} e^{-iZ_k \theta_k / 2} | G \rangle \\
&= \left(\bigotimes_{j \neq k} e^{-iZ_j \theta_j / 2} \right) \langle \pm | e^{iZ_k (\phi'_k + r_k \pi) / 2} | G \rangle \\
&= \left(\bigotimes_{j \neq k} e^{-iZ_j \theta_j / 2} \right) \langle \pm_{\phi'_k} | Z_k^{r_k} | G \rangle,
\end{aligned}$$

which means that Bob effectively does the $\{|\pm_{\phi'_k}\rangle\}$ basis measurement with the error Z^{r_k} . The error Z^{r_k} just flips the bit of the measurement result, and therefore it can be compensated later.

It was also shown that the protocol is blind [3]. Here, blind intuitively means that whatever Bob does, Bob cannot learn anything about Alice's input, output, and algorithm. Intuitive proof of the blindness is as follows: What Bob obtains are quantum states $\{|\pm_{\theta_j}\rangle\}_{j=1}^N$ and classical messages $\{\delta_j\}_{j=1}^N$. Hence Bob's state is

$$\sum_{\phi_1, \dots, \phi_N} \sum_{r_1, \dots, r_N} \bigotimes_{j=1}^N |+\phi'_j + r_j \pi\rangle \langle +\phi'_j + r_j \pi| = I^{\otimes N},$$

which means that Bob cannot learn anything about $\{\phi_j\}_{j=1}^N$ whichever POVM he does on his system.

In order to guarantee Alice's privacy, the geometry of the graph G must be secret to Bob. There are three ways of doing it. First one is to use the brickwork state [3]. It is a certain two-dimensional graph state which is universal with only $\{|\pm_{\theta}\rangle\}$ basis measurements for $\theta \in \{\frac{k\pi}{4} | k = 0, 1, \dots, 7\}$. Second one is to implant a "hair" to each qubit of the regular lattice graph state [8]. For example, let us consider the left graph state of Fig. 3. We can simulate Z measurement and any $X - Y$ plane measurement on any blue qubit with only

$X - Y$ plane measurements on yellow and blue qubits. Hence we can “carve out” a specific graph state from the square lattice of blue qubits as is shown in the right of Fig. 3. Third one is so called “the graph hiding technique” [9]. By using this technique, Alice can have Bob prepare any graph state in such a way that Bob cannot learn the geometry of the graph. This technique is based on the simple idea that CZ does not create entanglement if one of the qubits is $|0\rangle$ or $|1\rangle$:

$$\begin{aligned} CZ(|\psi\rangle \otimes |+\rangle) &= CZ(|\psi\rangle \otimes |+\rangle), \\ CZ(|\psi\rangle \otimes |-\rangle) &= (I \otimes Z)CZ(|\psi\rangle \otimes |-\rangle), \\ CZ(|\psi\rangle \otimes |0\rangle) &= |\psi\rangle \otimes |0\rangle, \\ CZ(|\psi\rangle \otimes |1\rangle) &= Z|\psi\rangle \otimes |1\rangle. \end{aligned}$$

Therefore, if Alice hides several qubits in $|0\rangle$ or $|1\rangle$ into the set of qubits she initially sends to Bob, she can let Bob create her desired graph state. Since Bob cannot distinguish $|0\rangle$, $|1\rangle$, and eight $|+\theta\rangle$ states, Bob cannot know when he entangles qubits (Fig. 4).

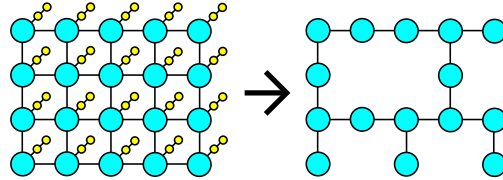


FIG. 3: (Color online.) The hair implantation technique [8]. Left: A two-qubit graph state (“hair”) indicated by yellow is attached to each blue qubit of the square graph state. Right: A desired graph state can be carved out from the blue square graph.

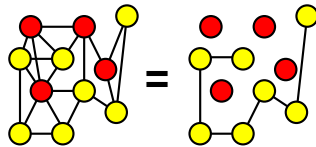


FIG. 4: (Color online.) The graph hiding technique [9]. Yellow qubits are $|+\theta\rangle$, whereas red qubits are $|0\rangle$ or $|1\rangle$. Bob applies CZ gates on all edges of the left graph, but actually he obtains the right graph state, and he does not know its geometry.

IV. CV BLIND PROTOCOL

Now let us consider the CV blind protocol. We here describe the ideal version and later consider realistic situations. Our protocol runs as follows:

1. Alice sends Bob

$$\left\{ S_q(-\theta_j) |0\rangle_p \right\}_{j=1}^N,$$

where $\theta_j = (a_j, b_j, c_j)$ is randomly chosen from \mathbb{R}^3 and $S_q(v) = F^\dagger R_q(v)$.

2. Bob applies CZ gates.
3. Alice and Bob might choose “the brickwork”, “the hair implantation technique”, or “the graph hiding technique”. Irrespective of their choice, we can assume without loss of generality that Bob has the “encrypted” CV graph state

$$\left[\bigotimes_{j=1}^N X^j(\xi_j) Z^j(\eta_j) S_q^j(-\theta_j) \right] |G\rangle,$$

where $|G\rangle$ is the N -qumode CV graph state, and the subscript j of X^j means it acts on the j th qumode.

4. For $j = 1$ to N in turn:

- (a) Let $\phi_j \equiv (\alpha_j, \beta_j, \gamma_j)$ be Alice’s computational parameters, and Let $\phi'_j \equiv (\alpha'_j, \beta'_j, \gamma'_j)$ be the one including feedforwardings. Alice sends Bob $\delta_j = M_{\xi_j}^{-1} w_j$ where

$$w_j = \begin{pmatrix} \alpha'_j + a_j - \eta_j + r_j \\ \beta'_j + b_j \\ \gamma'_j + c_j \end{pmatrix}$$

and $r_j \in \mathbb{R}$ is a random real number.

- (b) Bob applies $S_q(\delta_j)$ on j th qumode and does the p measurement on it. (Or he directly measures $S_q^\dagger(\delta_j) p S_q(\delta_j)$ of the j th qumode.) He sends the measurement result to Alice.

V. CORRECTNESS

Let us show the correctness of our protocol. See Fig. 2 (b), which is the circuit representation of our protocol. Since S_q commutes with CZ , Fig. 2 (b) is equivalent to Fig. 2 (a). Note that the equivalence between (a) and (b) in Fig. 2 is based on only the commutativity between S_q and CZ , and therefore it holds even if we replace each input $|0\rangle_p$ with its finitely squeezed version. Hence, the finite squeezing does not cause any additional effect here.

More precisely, note that the following is true for any state $|\psi\rangle$:

$$\begin{aligned}
& {}_p\langle p|S_q^j(\delta_j)X^j(\xi_j)Z^j(\eta_j)S_q^j(-\theta_j)|\psi\rangle \\
&= {}_p\langle p|X^j(\xi_j)Z^j(\eta_j)S_q^j(M_{\xi_j}M_{\xi_j}^{-1}w_j)S_q^j(-\theta_j)|\psi\rangle \\
&= {}_p\langle p|X^j(\xi_j)Z^j(\eta_j)S_q^j(w_j)S_q^j(-\theta_j)|\psi\rangle \\
&= {}_p\langle p|\exp\left[i\left\{(\alpha'_j + a_j - \eta_j + r_j)q + (\beta'_j + b_j)\frac{q^2}{2} + (\gamma'_j + c_j)\frac{q^3}{3} \right. \right. \\
&\quad \left. \left. + \eta_j q - a_j q - b_j \frac{q^2}{2} - c_j \frac{q^3}{3}\right\}\right]|\psi\rangle \\
&= {}_p\langle p|\exp[ir_j q]\exp\left[i\left\{\alpha'_j q + \beta'_j \frac{q^2}{2} + \gamma'_j \frac{q^3}{3}\right\}\right]|\psi\rangle \\
&= {}_p\langle p|\exp[ir_j q]S_q^j(\phi'_j)|\psi\rangle \\
&= {}_p\langle p - r_j|S_q^j(\phi'_j)|\psi\rangle.
\end{aligned}$$

Hence, Bob effectively does the correct MBQC except for the fact that if the measurement result is p , the byproduct which comes from this measurement is not $X(p)$ but $X(p - r_j)$, which can be compensated by changing the following measurement parameters. Since the above equation is true for any state $|\psi\rangle$, the situation does not change even if the squeezing is finite.

The brickwork implementation for the CV blind protocol is shown in Fig. 5, 6, and 7. Since $CZ \cdot CZ \neq I$ for the CV case, we cannot directly generalize the qubit brickwork state of Ref. [3]. In particular, we need CZ and CZ^\dagger as is shown in Figs. 5, 6, and 7.

The hair implantation technique also works if we implant four-qumode hair on each qumode, since the measurement of q on a qumode in a CV graph state removes that qumode [22], and a q measurement can be simulated only with $S_q^\dagger p S_q$ measurements by

using the following relations:

$$\begin{aligned} F \cdot F e^{iq^2/2} \cdot F e^{iq^2/2} \cdot F &= e^{iq^2/2} e^{ip^2/2}, \\ e^{-ip^2/2} e^{-iq^2/2} p e^{iq^2/2} e^{ip^2/2} &= q. \end{aligned}$$

The graph hiding technique for qubits can also be generalized to CV, since

$$\begin{aligned} CZ(|\psi\rangle \otimes |s\rangle_p) &= (I \otimes Z(s)) CZ(|\psi\rangle \otimes |0\rangle_p), \\ CZ(|\psi\rangle \otimes |s\rangle_q) &= (Z(s)|\psi\rangle) \otimes |s\rangle_q. \end{aligned} \tag{1}$$

Therefore, Alice can have Bob create a graph state where $Z(s)$ are applied on some qumodes in such a way that Bob cannot know the graph geometry.

Finally, let us consider the effect of the finite squeezing. As we have seen, the Alice's prerotation technique itself is valid for any initial state (Fig. 2), and therefore the finite squeezing does not cause any additional problem apart from the original one inherent to the non-blind CV MBQC [21, 22]. If Alice and Bob choose the brickwork implementation or the hair implantation technique, again the finite squeezing does not cause any additional effect since the brickwork blind quantum computation and the hair implantation technique are nothing but a normal cluster MBQC with some redundant gates. (Of course, this redundancy accelerates the accumulation of errors, and therefore requires more fault-tolerance, but such a problem is not a specific problem to the blind CV MBQC. Even the non-blind one ultimately needs enough fault-tolerance for the scalability [21, 22, 25, 29].) Finally, regarding the graph hiding technique, once the graph state is created, it is nothing but a usual CV MBQC with errors. If the squeezing is finite, Eq. (1) becomes not exact but approximate one. This causes additional errors on the created graph state, but such errors are that even the non-blind CV MBQC can experience.

VI. BLINDNESS

What Bob obtains are quantum states $\{S_q(-\theta_j)|0\rangle_p\}_{j=1}^N$ and classical messages $\{\delta_j\}_{j=1}^N$. Note that

$$\begin{aligned} \theta_j &= M_{\xi_j} \delta_j - \phi'_j + \eta_j e - r_j e \\ &\equiv k_j - r_j e, \end{aligned}$$

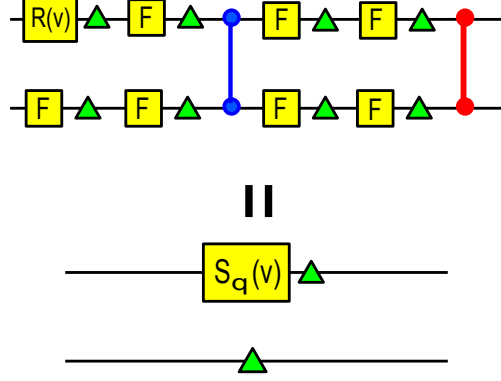


FIG. 5: (Color online.) The implementation of $S_q(v) \otimes I$. Blue two-qubit gate is CZ . Red two-qubit gate is CZ^\dagger . Green triangles are byproducts.

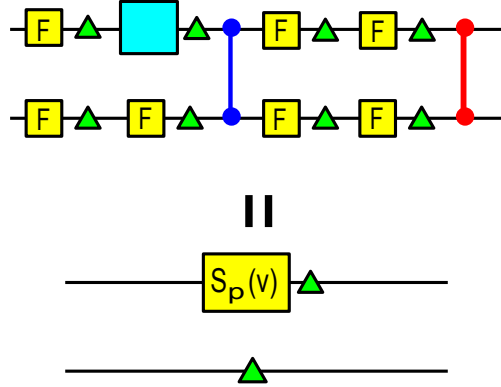


FIG. 6: (Color online.) The implementation of $S_p(v) \otimes I$. The blue box means $R_{-q}(M_m^{-1}v)$.

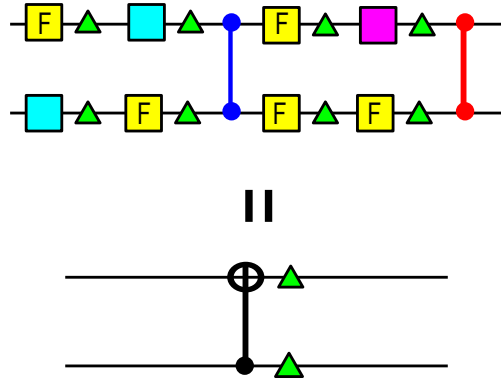


FIG. 7: (Color online.) The implementation of CX . The blue boxes are $Fe^{iq^2/2}$ up to byproduct corrections. The purple box is $Fe^{-iq^2/2}$ up to byproduct corrections.

where $e = (1, 0, 0)$. Hence, Bob's state is

$$\begin{aligned}
& \int \prod_{j=1}^N dr_j \bigotimes_{j=1}^N S_q(-\theta_j) |0\rangle_{pp} \langle 0| S_q^\dagger(-\theta_j) \\
&= \int \prod_{j=1}^N dr_j \bigotimes_{j=1}^N S_q(-k_j + r_j e) |0\rangle_{pp} \langle 0| S_q^\dagger(-k_j + r_j e) \\
&= \int \prod_{j=1}^N dr_j \bigotimes_{j=1}^N S_q(-k_j) e^{ir_j q} |0\rangle_{pp} \langle 0| e^{-ir_j q} S_q^\dagger(-k_j) \\
&= \int \prod_{j=1}^N dr_j \bigotimes_{j=1}^N S_q(-k_j) |r_j\rangle_{pp} \langle r_j| S_q^\dagger(-k_j) \\
&= I^{\otimes N},
\end{aligned}$$

which means that Bob's state is independent of $\{\phi_j\}_{j=1}^N$.

Note that the blindness holds also in the finite squeezed case, since

$$\begin{aligned}
& \int \prod_{j=1}^N dr_j \bigotimes_{j=1}^N S_q(-\theta_j) |0, \Omega_j\rangle_{pp} \langle 0, \Omega_j| S_q^\dagger(-\theta_j) \\
&= \int \prod_{j=1}^N dr_j \bigotimes_{j=1}^N S_q(-k_j + r_j e) |0, \Omega_j\rangle_{pp} \langle 0, \Omega_j| S_q^\dagger(-k_j + r_j e) \\
&= \int \prod_{j=1}^N dr_j \bigotimes_{j=1}^N S_q(-k_j) e^{ir_j q} |0, \Omega_j\rangle_{pp} \langle 0, \Omega_j| e^{-ir_j q} S_q^\dagger(-k_j) \\
&= \int \prod_{j=1}^N dr_j \bigotimes_{j=1}^N S_q(-k_j) e^{ir_j q} T_{\Omega_j} |0\rangle_{pp} \langle 0| T_{\Omega_j}^\dagger e^{-ir_j q} S_q^\dagger(-k_j) \\
&= \int \prod_{j=1}^N dr_j \bigotimes_{j=1}^N T_{\Omega_j} \left[S_q(-k_j) e^{ir_j q} |0\rangle_{pp} \langle 0| e^{-ir_j q} S_q^\dagger(-k_j) \right] T_{\Omega_j}^\dagger.
\end{aligned}$$

Here, the operator

$$T_\Omega \equiv \frac{1}{(\pi\Omega^2)^{1/4}} \int dt \ e^{-\frac{t^2}{2\Omega^2}} e^{iqt}$$

commutes with S_q .

VII. DISCUSSION

A. Implementation of $e^{iq^3/3}$

In optical systems, the implementation of $e^{iq^3/3}$ is much harder than those of e^{iq} and $e^{iq^2/2}$. Hence it would be desirable for Alice to avoid the implementation of $e^{iq^3/3}$ by herself.

There are two solutions. One is that Bob embeds many $e^{isq^3/3}|0\rangle_p$ with various s into his resource state. If Alice uses the hair implantation technique or the graph hiding technique, Bob cannot know which $e^{isq^3/3}|0\rangle_p$ contributes to the computation. The other is to use the relation

$$Q^\dagger(t)e^{i\gamma q^3/3}Q(t) = e^{i\gamma' q^3/3}, \quad (2)$$

where

$$Q(t) \equiv e^{-i \ln(t)(qp+pq)/2}$$

is the squeezing and $t = (\gamma'/\gamma)^{1/3}$. Since the squeezing can be done blindly, Alice can have Bob implement $e^{i\gamma' q^3/3}$ without allowing Bob to learn γ' .

B. Blind CV protocol for measuring Alice

If the state measurement is relatively easy, we can consider another blind quantum computation protocol, where Bob creates the resource state and Alice does the measurement [10]. One advantage of this protocol is that the security is guaranteed by the no-signaling principle [30], which is more fundamental than quantum physics, and Alice does not need to verify her measurement device (the device independence [31]). The CV cluster MBQC is suitable for such a measuring Alice protocol, since the measurements of

$$\begin{aligned} e^{-isq}pe^{isq} &= p + s, \\ e^{-isq^2/2}pe^{isq^2/2} &= p + sq \end{aligned}$$

are easily done with the homodyne detection. The gate $e^{isq^3/3}$ can be implemented blindly by using Eq. (2).

C. Temporal encoding

If we use the temporal degrees of freedom, only a single CZ machine is sufficient [32]. As is shown in Fig. 8, it is easy to see that blind versions of such a temporal encoding implementation are possible both for the preparing Alice (Fig. 8 (a)) and the measuring Alice (Fig. 8 (b)).

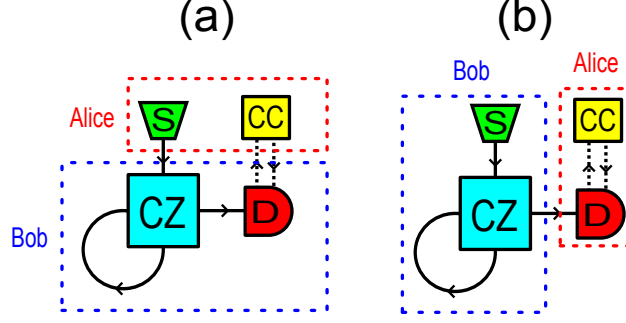


FIG. 8: (Color online.) Blind version of the temporal-encoding [32]. S is the squeezed state source, D is the measurement device, CZ is the machine which implements the CZ gate, and CC is a classical computer.

Acknowledgments

The author acknowledges JSPS for support.

Appendix A: Proof of Fig. 5

$$\begin{aligned}
& CZ^\dagger \begin{pmatrix} PF \cdot PF \\ PF \cdot PF \end{pmatrix} CZ \begin{pmatrix} PF \cdot PFS_q(v) \\ PF \cdot PF \end{pmatrix} \\
&= \begin{pmatrix} P \\ P \end{pmatrix} CZ^\dagger \begin{pmatrix} FF \\ FF \end{pmatrix} CZ \begin{pmatrix} FFS_q(v) \\ FF \end{pmatrix} \\
&= \begin{pmatrix} P \\ P \end{pmatrix} CZ^\dagger \begin{pmatrix} FFFF \\ FFFF \end{pmatrix} CZ \begin{pmatrix} S_q(v) \\ I \end{pmatrix} \\
&= \begin{pmatrix} P \\ P \end{pmatrix} \begin{pmatrix} S_q(v) \\ I \end{pmatrix},
\end{aligned}$$

where P is a byproduct and

$$\begin{aligned}
CZ^\dagger(X(m) \otimes I) &= (X(m) \otimes Z(-m))CZ^\dagger, \\
CZ^\dagger(I \otimes X(m)) &= (Z(-m) \otimes X(m))CZ^\dagger.
\end{aligned}$$

Appendix B: Proof of Fig. 6

$$\begin{aligned}
& CZ^\dagger \begin{pmatrix} PF \cdot PF \\ PF \cdot PF \end{pmatrix} CZ \begin{pmatrix} PFS_{-q}(M_m^{-1}v) \cdot X(m)F \\ PF \cdot PF \end{pmatrix} \\
&= \begin{pmatrix} P \\ P \end{pmatrix} CZ^\dagger \begin{pmatrix} FF \\ FF \end{pmatrix} CZ \begin{pmatrix} FS_{-q}(v)F \\ FF \end{pmatrix} \\
&= \begin{pmatrix} P \\ P \end{pmatrix} CZ^\dagger \begin{pmatrix} FFFF \\ FFFF \end{pmatrix} CZ \begin{pmatrix} S_p(v) \\ I \end{pmatrix} \\
&= \begin{pmatrix} P \\ P \end{pmatrix} \begin{pmatrix} S_p(v) \\ I \end{pmatrix}.
\end{aligned}$$

Appendix C: Proof of Fig. 7

$$\begin{aligned}
& CZ^\dagger \begin{pmatrix} X_g F e^{-i(q-h+c+b)^2/2} \cdot X_h F \\ X_f F \cdot X_e F \end{pmatrix} CZ \begin{pmatrix} X_d F e^{i(q-c)^2/2} \cdot X_c F \\ X_b F \cdot X_a F e^{iq^2/2} \end{pmatrix} \\
&= CZ^\dagger \begin{pmatrix} X_g e^{-i(p-h+c+b)^2/2} F X_h F \\ X_f Z_e F F \end{pmatrix} CZ \begin{pmatrix} F Z_{-d} X_c e^{iq^2/2} F \\ F Z_{-b} F Z_{-a} e^{iq^2/2} \end{pmatrix} \\
&= CZ^\dagger \begin{pmatrix} X_g e^{-i(p-h+c+b)^2/2} Z_h F F \\ X_f Z_e F F \end{pmatrix} CZ \begin{pmatrix} F F X_{-d} Z_{-c} e^{ip^2/2} \\ F F X_{-b} Z_{-a} e^{iq^2/2} \end{pmatrix} \\
&= CZ^\dagger \begin{pmatrix} X_g e^{-i(p-h+c+b)^2/2} Z_h \\ X_f Z_e \end{pmatrix} CZ \begin{pmatrix} X_{-d} Z_{-c} e^{ip^2/2} \\ X_{-b} Z_{-a} e^{iq^2/2} \end{pmatrix} \\
&= CZ^\dagger \begin{pmatrix} X_g e^{-i(p-h+c+b)^2/2} Z_h X_{-d} Z_{-c} Z_{-b} \\ X_f Z_e Z_{-d} X_{-b} Z_{-a} \end{pmatrix} CZ \begin{pmatrix} e^{ip^2/2} \\ e^{iq^2/2} \end{pmatrix} \\
&= CZ^\dagger \begin{pmatrix} X_g Z_h X_{-d} Z_{-c} Z_{-b} e^{-ip^2/2} \\ X_f Z_e Z_{-d} X_{-b} Z_{-a} \end{pmatrix} CZ \begin{pmatrix} e^{ip^2/2} \\ e^{iq^2/2} \end{pmatrix} \\
&= \begin{pmatrix} P \\ P \end{pmatrix} CZ^\dagger \begin{pmatrix} e^{-ip^2/2} \\ I \end{pmatrix} CZ \begin{pmatrix} e^{ip^2/2} \\ e^{iq^2/2} \end{pmatrix} \\
&= \begin{pmatrix} P \\ P \end{pmatrix} CX,
\end{aligned}$$

where

$$\begin{aligned}
(e^{-ip^2/2} \otimes I) e^{iq \otimes q} (e^{ip^2/2} \otimes I) &= e^{i(q \otimes q) - i(p \otimes q)} \\
&= e^{i(q \otimes q)} e^{-i(p \otimes q)} (I \otimes e^{-iq^2/2})
\end{aligned}$$

and we have used $e^{A+B} = e^A e^B e^{-[A,B]/2}$ which is valid if $[A, [A, B]] = [B, [A, B]] = 0$.

-
- [1] A. Childs, Quant. Inf. Compt. **5**, 456 (2005).
 - [2] P. Arrighi and L. Salvail, Int. J. Quant. Inf. **4**, 883 (2006).
 - [3] A. Broadbent, J. Fitzsimons, and E. Kashefi, Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science 517 (2009).

- [4] D. Aharonov, M. Ben-Or, and E. Eban, Proceedings of Innovations in Computer Science 453 (2010).
- [5] T. Morimae, V. Dunjko, and E. Kashefi, arXiv:1009.3486
- [6] V. Dunjko, E. Kashefi, and A. Leverrier, Phys. Rev. Lett. **108**, 200502 (2012).
- [7] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, Science **335**, 303 (2012).
- [8] T. Morimae and K. Fujii, arXiv:1110.5460; to be published in Nature Communications.
- [9] J. F. Fitzsimons and E. Kashefi, arXiv:1203.5217
- [10] T. Morimae and K. Fujii, arXiv:1201.3966
- [11] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
- [12] R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003).
- [13] R. Raussendorf, Ph.D. thesis, Ludwig-Maximilians Universität München (2003).
- [14] I. Affleck, T. Kennedy, E. H. Lieb, and H. Tasaki, Comm. Math. Phys. **115**, 477 (1988).
- [15] G. K. Brennen and A. Miyake, Phys. Rev. Lett. **101**, 010502 (2008).
- [16] R. Raussendorf and J. Harrington, Phys. Rev. Lett. **98**, 190504 (2007).
- [17] R. Raussendorf, J. Harrington, and K. Goyal, New J. Phys. **9**, 199 (2007).
- [18] R. Raussendorf, J. Harrington, and K. Goyal, Ann. Phys. **321**, 2242 (2006).
- [19] Y. Li, D. E. Browne, L. C. Kwek, R. Raussendorf, and T. C. Wei, Phys. Rev. Lett. **107**, 060501 (2011).
- [20] K. Fujii and T. Morimae, Phys. Rev. A **85**, 010304(R) (2012).
- [21] N. C. Menicucci, P. van Loock, M. Gu, C. Weedbrook, T. C. Ralph, and M. A. Nielsen, Phys. Rev. Lett. **97**, 110501 (2006).
- [22] M. Gu, C. Weedbrook, N. C. Menicucci, T. C. Ralph, and P. van Loock, Phys. Rev. A **79**, 062318 (2009).
- [23] R. Ukai, S. Yokoyama, J. Yoshikawa, P. van Loock, and A. Furusawa, Phys. Rev. Lett. **107**, 250501 (2011).
- [24] Y. Miwa, R. Ukai, J. Yoshikawa, R. Filip, P. van Loock, and A. Furusawa, Phys. Rev. A **82**, 032305 (2010).
- [25] R. Ukai, N. Iwata, Y. Shimokawa, S. C. Armstrong, A. Politi, J. Yoshikawa, P. van Loock, and A. Furusawa, Phys. Rev. Lett. **106**, 240504 (2011).
- [26] M. Yukawa, R. Ukai, P. van Loock, and A. Furusawa, Phys. Rev. A **78**, 012301 (2008).

- [27] Y. Miwa, J. Yoshikawa, P. van Loock, and A. Furusawa, Phys. Rev. A **80**, 050303(R) (2009).
- [28] S. Lloyd and S. L. Braunstein, Phys. Rev. Lett. **82**, 1784 (1999).
- [29] M. Ohliger, K. Kieling, and J. Eisert, Phys. Rev. A **82**, 042336 (2010).
- [30] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).
- [31] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
- [32] N. C. Menicucci, X. Ma, T. C. Ralph, Phys. Rev. Lett. **104**, 250503 (2010).